Queen Mary
University of London

IT Services Policy

DG02 – Business Continuity Policy

Prepared by: < Shelim Miah>
Version: 2.0

Effective Date:	28/05/2018	Next Review:	28/05/2021

Reviewers:	**Kathy Whelan, IT Service Desk Manager** **Henrick Brogger, Head of Service Delivery** **Amit Patel, Head of Service Management** **Martin Evans, Head of Data Centre Services** **Jason Bunning, Interim AD for Applications** **David Boakes, Assistant Director IT Operations** **David Cooper, Head of Infrastructure Delivery**
Policy Owner:	
Name/Position	Rhys Davies, Chief Information Officer

Revision History

Version	Description	Author	Date
1	Initial version.	William Mordaunt	28/09/2010
1	Annual Review – No Change	Chris Day	27/05/2014
1.1	Updated, to change the review process	Shelim Miah	23/11/2015
1	Initial version.	William Mordaunt	28/09/2010
2.0	Transferred onto a Policy Template	Shelim Miah	22/03/2016
2.0	Reviewed	Shelim Miah	24/05/2018

Authorisation:	
Name / Position	**Rhys Davies / Chief Information Officer**
Signature	**R. Davies**
Date	**28.05.18**

CONTENTS

1 Policy Statement

1.1 This policy has been established to ensure that business continuity plans are developed and maintained in accordance with QMUL's business continuity strategy and or business needs.

1.2 Defining standards for the development and maintenance of business continuity plans that will allow the operational activities to continue in the event of a disaster.

1.3 The Policy aims to:

- Outline the expectations of business continuity co-ordinators.
- Ensure business continuity plans are in place.
- Ensure QMUL is able to operate and recover from a disaster
- Outline roles & responsibilities
- Enhance Communications

2 Scope

2.1 The policy applies to all staff and third parties suppliers who manage services on behalf of QMUL and all systems processes and procedures required for the day to day operation activities of QMUL.

3 Policy Detail

3.1 QMUL must appoint a suitably senior member of staff to perform the role of Business Continuity Manager (BCM).

3.2 The QMUL BCM will formulate and agree a business continuity strategy in line with the College's objectives and strategy.

3.3 The business continuity strategy must outline alternative operating methods to maintain or resume QMUL's core operational activities after an interruption or major failure of its critical systems, processes and services.

3.4 The business continuity strategy must address the vulnerabilities and single points of failure in QMUL's critical processes and any associated service.

3.5 Each Director/Head of Department need to identify a Business Continuity Coordinator (BCC) for their department. The individual must be at a suitably high level to embed the management of Business Continuity Plan (BCP) into the organisation.

3.6 The QMUL Business Continuity Manager/ Directors/ Heads of Department need to ensure that adequate resources (financial, organisational, technical, and environmental) are available to address the requirements of business continuity planning.

3.7 A business impact analysis must be conducted by the BCC, which will identify the business processes performed by the directorate or department and its criticality. For examples; paying suppliers, providing a potable water supply, providing an e-mail service, etc.

3.8 For each process and any associated service, the maximum tolerable period of disruption (MTPD) must be identified. The MTPD is the maximum length of time that a service can be unavailable before irreparable harm is caused.

3.9 The BCC within each directorate or department will be required to conduct a risk analysis for each process, focussing on the most critical ones identified in the business impact analysis. Refer to SOP DG01 - Information Risk Assessments.

3.10 The BCC within each directorate or department will need to formulate and document detailed business continuity plans (BCP) that are consistent with the QMULs Business Continuity strategy.

3.11 The BCP must reduce the likelihood of specific threats identified in the risk analysis and Mitigation/Control measures to address the threats.

3.12 The Plan must also outline how situations resulting from risk events that impact critical processes are managed and include roles and responsibilities, notification, triggers for invoking of business continuity plans, assessment phase, recovery phase, through to return to normal operation. Plans need to include details of the resources required for execution, e.g. staff, skills, premises, technical, information, equipment, supplies, services and support from third parties.

3.13 The BCM must liaise with BCC to ensure that adequate training is provided for those persons involved in the execution of the BCP. Staff awareness training must also be provided to ensure that all staff are aware of BCP and how their roles may change if plans are invoked.

3.14 The BCP must be regularly tested. Testing may take a variety of forms, from desktop exercises to full testing of plans.

3.15 The BCP must be updated to incorporate lessons learned from testing and any changes to business processes, risks, impacts or the IT environment.

4 Process and Procedures

4.1 For any associated processes and guidance documents can be found by visiting the ITS webpage.

5 Roles & Responsibility

5.1 The Risk and Governance Manager will be responsible for initiating the review cycle for the policy, process document owner to carry out the review. The Document owner will assess and incorporate any comments or feedback received.

5.2 Once the document has been updated, the Risk and Governance Manager will take the document to the appropriate approval body for approval. All approved documentation are to be stored in a central repository and uploaded to the web where applicable.

6 Monitoring

6.1 It is mandatory for all staff and third parties suppliers who manage services on behalf of QMUL comply with this IT Policy and any associated procedure. Where non-compliance is identified, ITS will take appropriate action.

6.2 Checks will be made by the Risk and Governance Manager and the findings will be reported to the IT Lead Team (ITLT) in the first instance for corrective actions to be issued.

6.3 The AD of IT Operations, in conjunction with the Risk & Governance Manager, is responsible for the monitoring, revision and updating of this policy.

7 Exceptions

7.1 In the event of an exception that is not addressed by this policy, the matter will be firstly referred to the ITLT via the Assistant Director for IT Operations.

7.2 The ITLT will then make a decision or refer this to the IT Strategy Board (ITSB) for further guidance as necessary.

8 References

SOP DG00 - Review and Update of Policies & Standard Operating Procedures

9 Appendix A - Definitions

Term	Meaning
Approval Body	May refer to where appropriate the Information Governance Group, IT Lead Team or any other board/group owning the policy.
Risk	A Risk can be anything (an action, event or set of circumstances) that can adversely or beneficially affect QMUL's ability to achieve its current or future objectives
BCM	Business Continuity Manager, a role that is charged with developing the strategy to ensure the organisation can still operate in the event of a disaster or at the least, the impact is minimised.
BCP	Business Continuity plan, this details the processes that to be enacted detailing what tasks are carried out by who and when in the event of a disaster.
MTPD	Maximum tolerable period of disruption is the maximum length of time that a service can be unavailable before irreparable harm is caused to QMUL
User	A member of staff, enrolled student, contractor, visitor, or another (any other) person authorised to access and use QMUL's systems.
ITLT	IT Lead Team – Team of Senior Managers consisting of the Assistant Directors of IT, Faculty Relationship Managers and Chaired by the IT Director.
ITSB	IT Strategy Board – Team of Executive Managers consisting of Vice Principals and the IT Director, who oversee the delivery of the IT Strategy.